In the Specification:

Please substitute the following paragraph for **paragraph 5** on **page 13** of the application.

> It is noted that the audio file may not be transmitted directly to the content player 216 and the certificate entity 222 but may first pass through one or more intermediaries (not shown). In addition, the music provider 201 and the certificate entity 222 could be the same entity. In such a case, the content file is not transmitted to a certificate entity; instead, the certificate is produced and stored at the music provider 201. Typically, however, it is ~~anticipate~~ anticipated that a user will obtain the audio file from the music provider 201 and will then connect with the certificate entity 222 to obtain the certificate 220 associated with the audio file.

Please substitute the following paragraph for **paragraph 1** on **page 15** of the application.

> At block 320, the certificate entity 222 receives the certificate ~~requests~~ request and attempts to locate the certificate 220 (block 322). If the certificate 220 cannot be found ("No" branch, block 322), then an error message is produced at block 323 indicating that a valid certificate 220 associated with the marked content 214 could not be located. If the certificate 220 is located ("Yes" branch, block 322), then the certificate 220 is then transmitted to the content player 216 at block 324.

Please substitute the following paragraph for paragraph **2** on page **17** of the application.

> The content player 402 is configured to receive the content file 416' into the memory 404. When a request is made to process the content file 416', the authentication module 426 is configured to locate the certificate 418' that is associated with the content file 416'. In the present example, the ~~content file~~ certificate 418' is downloaded from the content owner site 414, although in one implementation, the certificate 418' is located and downloaded from the certificate entity 422. Once the certificate 418' has been stored in the memory 404, the authentication module 426 validates the contents of the certificate 418' and determines if the content player 402 is authorized to process the content file 416' in accordance with the request. If so, the content file 416' is processed as requested; if not, the content file 416' is not processed.